

Architecture & Cybersecurity - Module 4

- ELO-075** Identify cybersecurity concerns associated with a Cloud service offering at the Infrastructure, Network and Application Layers. Figure 1
- ELO-090** Identify the concerns for where the data the stored; the student will know the different ways of storing data (ELO-091).
- ELO-115** Match key cybersecurity terms from the section to appropriate definitions.

Module – 4: Arch & Cyber

Topics

- Module Introduction
- Recapitulation
- Cybersecurity for Infrastructure, Network and Application Layers
- Concerns for where the data the stored
- Module Review
- Module Summary Questions

You should be able to:

- Identify cybersecurity concerns associated with a Cloud service offering at the Infrastructure, Network and Application Layers
- Identify the concerns for where the data the stored;
- Identify the different ways of storing data
- Match foundational cloud terms from the section to appropriate definitions.

Recapitulation of Modules – 1, 2, 3

Topic

Content

Review Previous Content

You should be able to:

Questions

Cloud Cybersecurity Overview

Topic

Cloud Cybersecurity Overview

You should be able to:

1. (New MT) Identify key cybersecurity policy elements

Questions

Content

- Risk Management Framework (RMF)
- Provisional Authorization
- Risk Management tools
 - DOD Cloud Computing Security Requirements Guide (DISA) (http://iase.disa.mil/cloud_security/Pages/index.aspx)
 - Draft Cloud Access Point (CAP) Functional Requirements Document (FRD) V2.2 (http://iase.disa.mil/cloud_security/Pages/index.aspx)
 - Best Practices Guide for DoD Cloud Mission Owners (http://iase.disa.mil/cloud_security/Pages/index.aspx)

Cybersecurity for Infrastructure, Network and Application Layers

Topic

Cybersecurity for Infrastructure, Network and Application Layers

You should be able to:

1. MT-075-01 Identify different types of storage media

Questions

Content

- Cloud storage media includes network accessible storage, virtualized storage and various disc arrays
- The DOD Cloud Computing Security Requirements Guide (DISA) (http://iase.disa.mil/cloud_security/Pages/index.aspx) provides detailed implementation details for securing data at rest and transit.

Cybersecurity for Infrastructure, Network and Application Layers

Topic

Cybersecurity for Infrastructure, Network and Application Layers

You should be able to:

1. MT-075-02 Identify different ways cloud service providers store users data

Questions

Content

- Cloud storage is referred to in layers including, for example:
 - Objects – metadata and data organized as web-based content.
 - Datasets – organized data in relational or other record formats
 - Blocks – stored at the hardware level
 - this is the smallest element of data accessible by a user or other system
 - Files – data objects (documents, spreadsheets, pictures, etc.) organized into folders for easy visualization by users.

Cybersecurity for Infrastructure, Network and Application Layers

Topic

Cybersecurity for Infrastructure, Network and Application Layers

You should be able to:

1. MT-075-03 Identify different ways of protecting data

Questions

Content

- Data must be protected to maintain confidentiality and integrity.
 - Confidentiality is protection from unauthorized access by those without an appropriate security clearance and need to know.
 - Confidentiality is often protected with encryption, identity and access management and physical security measures (doors, guards, cameras, etc.)
 - Integrity is guarding against unwanted changes to data. For example Global Positioning System (GPS) data is protected from changes that would miss-identify locations.
 - The DOD Cloud Computing Security Requirements Guide (DISA) (http://iase.disa.mil/cloud_security/Pages/index.aspx) provides detailed implementation details for securing data at rest and transit.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-01 Identify the benefits and concerns with virtual servers

Questions

Content

- Virtual Servers enable flexible computing capacity on demand. Traditional, physical servers, required funding, purchase, receipt, mounting, configuration and maintenance for any hardware failures. Virtual Servers do not require setup or physical maintenance for the acquiring organization as the cloud provider takes care of everything from the hypervisor down through hardware.
- Virtual server concerns include
 - lack of trained workforce for cloud implementations.
 - Expectations that it will be considered a panacea for architecture issues in existing systems migrating to cloud.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-02 Identify the benefits and concerns with virtual networks

Questions

Content

- Virtual networks can be constructed and maintained without having to move physical links and cables.
- Traditional networks required significant planning for changes and, as a result, took a great deal of time to implement changes.
- Virtual networks still require planning for secure implementation but do not require changing cable and physical router changes.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-03 one benefit of virtualization is sharing of resources (resources pooling/sharing)

Questions

Content

- Shared resources improve reliability and rapid access.
- Reliability is improved when shared storage is maintain across physical servers in redundant configurations so that a failed hard drive can be replaced without any interruption in service.
- For example storage across multiple machines using Hadoop stores information on 3 separate machines so that failure of 1 of 3 can be repaired without bringing down applications. The new hard drive is inserted and the cloud instance automatically configures it to replace the failed drive.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-04 supports elasticity

Questions

Content

- Virtualized data storage can be configured to expand based on the needs of the system being supported.
- For example if an application or user requires an initial storage level of 100 GB but is expected to increase to 1TB over the course of a year the provider can set the storage to expand as it is needed. This avoids purchasing more storage than required as would be the case with traditional hardware storage.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-05 supports automation

Questions

Content

- Virtualization supports many automation capabilities to enable stand up of new virtual machines.
- Using automatically configured systems reduces the time to implement and the likely hood of miss-configured systems.
- Automation can also audit virtual machines, networks and storage to ensure cybersecurity postures are maintained and kept up to date.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-06 concerns - security

Questions

Content

- Data storage Cybersecurity concerns generally fall into two categories. The first is the location of the physical hardware globally and the second is the configuration within a data center.
- Global location of the cloud data center is a concern because of local laws that may impact the confidentiality of the system. Some contrives require access to any data on their soil. Generally DoD Clouds can only be located on US soil in the US.
- Configuration in the data center includes physical separation to mitigate risks including vulnerabilities in interfaces, APIs and management systems.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-07 physical hardware

Questions

Content

- Physical hardware includes all of the equipment provided or used by the cloud service provider.
- Examples include building, cooling system, power, network connectivity, server racks, servers, switches and other equipment required to support a virtualized environment.
- DOD must be prepared for threats that include cross talk across networks and environments. In some cases, including classified systems, servers, routers and cabling must be physically separated. Examples include separation of classified systems onto different physical networks known as “air gapping”.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-09 requires less people, increases ability to manage more machines

Questions

Content

- Physical systems often require staff be collocated to conduct maintenance on the hardware and software. This included the need to physically press a button to restart a machine.
- Virtualization allows systems owners and administrators to access systems remotely to build, deploy and maintain them. This can include remote restarts of virtual machines and remote metrics visibility.
- Remote management can improve response times to security events and it can reduce the cost of having dedicated collocated staff.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-09 requires less people, increases ability to manage more machines

Questions

Content

- Physical servers and infrastructure often are managed locally. An administrator would go into the server room and log in at the actual machine. This was time consuming and expensive.
- Virtualized servers can be accessed remotely thus reducing time spent working on a single machine and thus making management more efficient. An administrator can log in remotely to address any security concerns or issues.
- This virtualized, remote access, improves response time to security incidents and can reduce the time required to mitigate vulnerabilities.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-10 standardization - each virtual machine is the same therefore easier to manage

Questions

Content

- Physical machine implementation is often inefficient because the hardware had to be ordered, installed, configured and managed for each server.
- Virtualized machines can be standardized into prepackaged installs that can be automatically implemented.
- This approach provides a level of standardization that makes implementation much faster and easier to operate.
- For example DISA and others have standardized templates for new virtual machines to make it easier to rapidly deploy the desired configuration.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-11 concern- performance due to sharing of resources

Questions

Content

- Virtual machines are efficient because they share resources. This, however; can lead to resource constraints outside of the systems administrators control.
- For example, if one organization has virtualized their public facing web site on the same infrastructure as a commercial news service. These are logically and virtually separated but they are on the same infrastructure. In this case when a hot news story drive large data flow and processing from the news site the host may reduce the performance to the command site.
- This is referred to as the noisy neighbor problem.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-12 faster redeployment as a result of standardization

Questions

Content

- Because cloud instances can be stood up without needing to go through the lengthy process of ordering, installing and configuring bare hardware. This results in a significant reduction labor and time needed in the tasks required by systems owners.
- Standardized VMs can improve security and accreditation because of their standardization. This way if a bug is identified it can be mitigated with the minimum time available.

Data Storage Cybersecurity

Topic

Data Storage Cybersecurity

You should be able to:

1. MT-090-13 faster back-up and recovery due to standardization

Questions

Content

- Cloud implementations and their associated data can be configured to speed backup and recovery.
- Virtual machines or groups of these machines can be automatically backed up to physically distant data centers where common hosting environments can spin up quickly. This approach leveraged the ability to abstract the hypervisor layer and the ability to take data snapshots for backups.
- Depending on the configurations, standardized machines can be implemented as hot sites with load balancing across sites. This approach allows for fail over of a site without impacting the enterprise.

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-01 Match Hybrid Cloud to the correct definition

Questions

Content

- **Hybrid Cloud:** A hybrid cloud is an infrastructure that includes links between one cloud managed by the user (typically called “private cloud”) and at least one cloud managed by a third party (typically called “public cloud”). Although the public and private segments of the hybrid cloud are bound together, they remain unique entities. This allows a hybrid cloud to offer the benefits of multiple deployment models at once. Hybrid clouds vary greatly in sophistication. For example, some hybrid clouds offer only a connection between the on premise and public clouds. All the difficulties inherent in the two different infrastructures is the responsibility of operations and application teams. (<http://appenda.com/library/glossary/hybrid-clouds-a-definition/>)

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-02 Match Hypervisor to the correct definition
2. MT-115-03 Match Lights-Out Data Center to the correct definition

Questions

Content

- A **hypervisor** is a piece of computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine. Each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. (<https://en.wikipedia.org/wiki/Hypervisor>)
- A **lights out data center** is a server or computer room that is physically or geographically isolated at an organization's headquarters, thereby limiting environmental fluctuations and human access. Unnecessary energy used for lighting and for maintaining a proper climate around frequently used doors can be saved by going lights out. (<https://www.techopedia.com/definition/26965/lights-out-data-center>)

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-04 Match Multi-Tenancy to the correct definition

Content

- Multi-tenancy is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant. Tenants may be given the ability to customize some parts of the application, such as color of the user interface (UI) or business rules, but they cannot customize the application's code.
- Multi-tenancy can be economical because software development and maintenance costs are shared. It can be contrasted with single-tenancy, an architecture in which each customer has their own software instance and may be given access to code. With a multi-tenancy architecture, the provider only has to make updates once. With a single-tenancy architecture, the provider has to touch multiple instances of the software in order to make updates.
- In cloud computing, the meaning of multi-tenancy architecture has broadened because of new service models that take advantage of virtualization and remote access. A software-as-a-service (SaaS) provider, for example, can run one instance of its application on one instance of a database and provide web access to multiple customers. In such a scenario, each tenant's data is isolated and remains invisible to other tenants.
- (<http://whatis.techtarget.com/definition/multi-tenancy>)

Questions

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-05 Match Physical Separation to the correct definition

Questions

Content

- While shared cloud environments provide significant opportunities for DoD entities, they also present unique risks to DoD data and systems that must be addressed. These risks include UNCLASSIFIED exploitation of vulnerabilities in virtualization technologies, interfaces to external systems, APIs, and management systems. These have the potential for providing back door connections and CSP privileged user access to customer's systems and data (insider threat). While proper configuration of the virtual and physical environment can mitigate many of these threats, there is still residual risk that may or may not be acceptable to DoD. Legal concerns such as e-discovery and law enforcement seizure of non-government CSP customer/tenant's data pose a threat to DoD data if it is in the same storage media. Due to these concerns, DoD is currently taking a cautious approach with regard to Level 5 information. (DoD CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG) Version 1, Release 1 12 January 2015 page 24-25)

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-06 Match Software-Defined Networking (SDN) to the correct definition

Questions

Content

- Software-defined networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center. The goal of SDN is to allow network engineers and administrators to respond quickly to changing business requirements. In a software-defined network, a network administrator can shape traffic from a centralized control console without having to touch individual switches, and can deliver services to wherever they are needed in the network, without regard to what specific devices a server or other device is connected to. The key technologies are functional separation, network virtualization and automation through programmability. (<http://searchsdn.techtarget.com/definition/software-defined-networking-SDN>)

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-07 Match Virtual Machine to the correct definition

Questions

Content

- A virtual machine (VM) is a software implementation of a machine (for example, a computer) that executes programs like a physical machine. Virtual machines are separated into two major classes, based on their use and degree of correspondence to any real machine: A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS). [1] These usually emulate an existing architecture, and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use (for example, executing on otherwise obsolete platforms), or of having multiple instances of virtual machines leading to more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization, the key to a cloud computing environment), or both.
- A process virtual machine (also, language virtual machine) is designed to run a single program, which means that it supports a single process. Such virtual machines are usually closely suited to one or more programming languages and built with the purpose of providing program portability and flexibility (amongst other things). An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine—it cannot break out of its virtual environment.

Key Cybersecurity Terms

Topic

ELO-115 Match key cybersecurity terms from the section to appropriate definitions.

You should be able to:

1. MT-115-08 Match Virtualization to the correct definition
2. MT-115-09 Match Virtual Separation to the correct definition

Questions

Content

- **Virtualization** refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources. (<https://en.wikipedia.org/wiki/Virtualization>)
- **Virtual Separation:** The risks and legal considerations in using virtualization technologies further restrict the types of tenants that can obtain cloud services from a virtualized environment on the same physical infrastructure and the types of cloud deployment models (i.e., public, private, community, and hybrid) in which the various types of DoD information may be processed or stored.

While shared cloud environments provide significant opportunities for DoD entities, they also present unique risks to DoD data and systems that must be addressed. These risks include exploitation of vulnerabilities in virtualization technologies, interfaces to external systems, APIs, and management systems.

These have the potential for providing back door connections and CSP privileged user access to customer's systems and data (insider threat). While proper configuration of the virtual and physical environment can mitigate many of these threats, there is still residual risk that may or may not be acceptable to DoD.

Module 4 - Review

Topic

Content

Summary

You should be able to:

Questions

Module 4 – Summary Questions

Topic

Content

Summary

You should be able to:

Questions